Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

A PROPERTY OF CYCLOTOMIC INTEGERS AND ITS RELATION TO FERMAT'S LAST THEOREM.*

BY H. S. VANDIVER.

If p is an odd prime, and

$$x^p + y^p + z^p = 0 \tag{1}$$

is satisfied in rational integers prime to each other then Furtwängler[†] has shown that

$$\frac{r^{p-1}-1}{p} = q(r) \equiv 0 \pmod{p},$$

for each factor r of x in case $x \not\equiv 0 \pmod{p}$ and for each factor r of $x^2 - y^2$ in case $x^2 - y^2$ is prime to p. Kummer[‡] showed that if (1) is satisfied in integers prime to each other and to p, then

$$B_n \left[\frac{d^{p-2n} \log (x + e^v y)}{dv^{p-2n}}\right]_{v=0} \equiv 0 \pmod{p}, \tag{1a}$$

where $B_1 = 1/6$, $B_2 = 1/30$, $\cdots$ are the numbers of Bernoulli, and $n = 1, 2, 3, \cdots (p-3)/2$. Mirimanoff[§] proved that these criteria may be replaced by

$$B_n f_{p-2n}\left(-\frac{x}{y}\right) \equiv 0 \pmod{p}, \qquad \left(n = 1, 2, 3, \cdots \frac{p-3}{2}\right),$$

where

$$f_i(t) = t + 2^{i-1}t^2 + \cdots + (p-1)^{i-1}t^{p-1}.$$

In the present paper I shall derive the above results by methods a bit different from those employed by the writers mentioned, as well as some other criteria in reference to (1). It is shown that the criteria of Kummer and Furtwängler may all be derived from one relation.

1. Kummer[||] proved that if $\mathfrak{P}$ is a prime ideal of the first degree in the algebraic field defined by $\alpha = e^{2i\pi/p}$ $(i = \sqrt{-1})$, then $\Pi_q \Pi_s \mathfrak{P}_{[1:s]}$ is a principal ideal in $\Omega(\alpha)$ where s ranges over the integers which satisfy

$$\frac{qp}{k+1} < s < \frac{qp}{k},$$

---

* Presented to the American Mathematical Society, Dec. 1914.

[†] Sitsungsberichte K. Akademie der Wissenschaften, Wien, vol. 121 (1912), p. 589.

[‡] Abhandlungen der K. Akademie der Wissenschaften zu Berlin, 1857.

[§] Journal für die Mathematik, vol. 128, pp. 45–68.

[||] Journal für die Mathematik, vol. 35, p. 364.

q ranges over the set 1, 2, $\cdots$, k, and k is any integer subject to the conditions $0 < k < p - 1$. Further $\mathfrak{P}_a$ is the ideal obtained from $\mathfrak{P}$ by the substitution (α/α^a) and $[1 : s]$ is the least positive solution of $sX \equiv 1 \pmod{p}$. In Hilbert's* notation this may be expressed

$$\prod_q \prod_s \mathfrak{P}_{[1:s]} \sim 1. \tag{2}$$

Let $k = 1$, the relation becomes

$$\prod_{s=(p+1)/2}^{p-1} \mathfrak{P}_{[1:s]} \sim 1. \tag{2a}$$

Let $k = 2$ in (2) and multiply the resulting relation by (2a). The product may be written

$$\prod_{\nu=1}^{2} \prod_{r=[\nu p/3]+1}^{p-1} \mathfrak{P}_{[1:r]} \sim 1. \tag{2b}$$

Using the substitution (α/α^{p-1}), we get

$$\prod_{\nu=1}^{2} \prod_{r=1}^{[\nu p/3]} \mathfrak{P}_{[1:r]} \sim 1.$$

In like manner, comparison of (2b) with (2) for $k = 3$ gives

$$\prod_{\nu=1}^{3} \prod_{r=1}^{[\nu p/4]} \mathfrak{P}_{[1:r]} \sim 1,$$

and we find in general

$$\prod_{\nu=1}^{k-1} \prod_{r=1}^{[\nu p/k]} \mathfrak{P}_{[1:r]} \sim 1 \qquad (k = 2, 3, \cdots, p - 1). \tag{3}$$

2. If $z \not\equiv 0 \pmod{p}$, we obtain from (1)

$$x + y = w^p, \qquad (w, \text{ an integer}) \tag{4}$$

$$x + \alpha y = \mathfrak{q}^p, \tag{5}$$

where $\mathfrak{q}$ is an ideal in the field $\Omega(\alpha)$. If $\mathfrak{q}_s$ denotes the ideal obtained from $\mathfrak{q}$ by the substitution (α/α^s), we have from (5)

$$\Pi'((x + \alpha^{[1:r]}y)) = \Pi'\mathfrak{q}^p_{[1:r]},$$

if

$$\Pi' = \prod_{\nu=1}^{k-1} \prod_{r=1}^{[\nu p/k]}$$

Since $\mathfrak{q}$ contains as factors only ideals of the first degree, the relation (3) gives

$$\Pi'(x + \alpha^{[1:r]}y) = \epsilon(\alpha)\theta^p, \tag{6}$$

where $\epsilon(\alpha)$ is a unit and θ is an integer in $\Omega(\alpha)$. Using the substitution (α/α^{-1}), we get

$$\Pi'(x + \alpha^{-[1:r]}y) = \epsilon(\alpha^{-1})\theta^p_{-1}. \tag{6a}$$

Now (1), (4), (6) and (6a) show that the ideal $(\theta\theta_{-1}) = ((-z/w)^{k-1})$, and therefore $\theta\theta_{-1} = E(-z/w)^{k-1}$, where E is a unit in Ω. The product of (6) and (6a) then gives

---

* Bericht der Deutschen Mathematiker Vereinigung, 1894, p. 223.

$$(7) \qquad \epsilon(\alpha)\epsilon(\alpha^{-1})E^p = 1.$$

But we also have

$$(7a) \qquad \epsilon(\alpha) = \alpha^q\epsilon'(\alpha + \alpha^{-1}),^*$$

$\epsilon'(\alpha + \alpha^{-1})$ denoting a unit in the field defined by $\alpha + \alpha^{-1}$ From (7) and (7a) we obtain $(\epsilon'(\alpha + \alpha^{-1}))^2 = E^{-p}$, and if s and r are integers such that $2s = 1 + rp$, then

$$\epsilon'^{2s} = \epsilon'\epsilon'^{rp} = E^{-sp}$$

and $\epsilon' = E_1{}^p$, where E_1 is a unit in Ω. Hence $\epsilon = E_1{}^p\alpha^g$, and we obtain

$$(8) \qquad \alpha^{-g}\Pi'(x + \alpha^{[1:r]}y) = \omega^p$$

Now by following a method employed by Kummer in the article cited, any integral relation between the pth roots of unity, say

$$f(\alpha) = 0,$$

may be replaced by

$$f(u) = F(u)\frac{u^p - 1}{u - 1},$$

where u is an arbitrary magnitude and $F(u)$ is an integral function of u. Applying this principle to (8), we obtain

$$(9) \qquad u^{-g}\Pi'(x + u^{[1:r]}y) = (\omega(u))^p + V(u)\frac{u^p - 1}{u - 1},$$

where $V(u)$ is an integral function of u. Setting $u = e^v$, we obtain from (9)

$$-vg + \sum_{\nu, r} \log(x + e^{v[1:r]}y) = \log(\omega^p + VX),$$

where

$$X = \frac{e^{vp} - 1}{e^v - 1}$$

Put $[1 : r] = n_r$. Differentiation gives

$$(10) \qquad -g + \sum_{\nu, r}\frac{d\log(x + e^{vn_r}y)}{dv} = \frac{d\log(\omega^p + VX)}{dv}$$

Let $v = 0$, we get

$$(10a) \qquad \begin{aligned} -g + \frac{y}{x + y}\sum_{\nu, r} n_r &= \left[\frac{d\log(\omega^p + VX)}{dv}\right]_{v=0} \\ &= \left[\frac{1}{\omega^p + VX}\left(\frac{p\omega^{p-1}d\omega}{dv} + \frac{dVX}{dv}\right)\right]_{v=0} \end{aligned}$$

Now $[\omega^p + VX]_{v=0}$ is prime to p, since ω is prime to p. Further

$$\left[\frac{dVX}{dv}\right]_{v=0} \equiv 0 \pmod{p},$$

---

* Hilbert, l. c., p. 336.

since $[X]_{v=0} = p$, and

$$\left[\frac{dX}{dv}\right]_{v=0} = 1 + 2 + 3 + \cdots + p - 1.$$

Hence

$$-g + \frac{y}{x+y}\sum_{v,r} n_r \equiv 0 \pmod{p}. \tag{11}$$

We note further that

$$\left[\frac{d^hX}{dv^h}\right]_{v=0} = 1 + 2^h + \cdots + (p-1)^h \equiv 0 \pmod{p},$$

for $0 < h < p - 1$. We therefore find

$$\left[\frac{d^h \log (\omega^p + VX)}{dv^h}\right]_{v=0} \equiv 0 \pmod{p},$$

since $[\omega^p + VX]_{v=0}$ is prime to p. Differentiation of (10) then gives

$$\sum_{v,r} n_r^h \left[\frac{d^h \log (x + e^v y)}{dv^h}\right]_{v=0} \equiv 0 \pmod{p}, \tag{12}$$

for $h = 2, 3, \cdots, p - 2$. We have, evidently,

$$\sum_{v,r} n_r^h \equiv \sum_{v=1}^{k-1} \sum_{j=1}^{[vp/k]} \frac{1}{j^h} \pmod{p}. \tag{13}$$

Now if $-y/x = t$ ($x \not\equiv 0 \pmod{p}$), then

$$\frac{d \log (x + e^v y)}{dv} = -\frac{te^v}{1 - te^v}.$$

We note that

$$\frac{d}{dv}\left(\frac{s}{1-s}(s^p - 1)\right) = (s^p - 1)\frac{d}{dv}\left(\frac{s}{1-s}\right) + \frac{s}{1-s}\frac{d}{dv}(s^p - 1),$$

where $s = e^v t$. Hence*

$$\left[\frac{d}{dv}\left(\frac{s(s^p-1)}{1-s}\right)\right]_{v=0} \equiv \left[(s^p - 1)\frac{d}{dv}\left(\frac{s}{1-s}\right)\right]_{v=0} \pmod{p},$$

since $1 - t$ is prime to p.

Proceeding in this way we find

$$\left[\frac{d^{a-1}}{dv^{a-1}}\left(\frac{s(s^p-1)}{1-s}\right)\right]_{v=0} \equiv (t^p - 1)\left[\frac{d^{a-1}}{dv^{a-1}}\left(\frac{s}{1-s}\right)\right]_{v=0}$$

modulo p. Or

$$f_a(t) = t + 2^{a-1}t^2 + \cdots + (p-1)^{a-1}t^{p-1}$$
$$\equiv -(t^p - 1)\left[\frac{d^{a-1}}{dv^{a-1}}\left(\frac{s}{1-s}\right)\right]_{v=0} \pmod{p}.$$

---

* Frobenius, Berlin Sitsungsberichte, July, 1910, p. 843.

Applying this to (12) and (13), we obtain

$$\sum_{\nu=1}^{k-1} \sum_{j=1}^{[\nu p/k]} \frac{1}{j^a} f_a(t) \equiv 0 \pmod{p}, \tag{14}$$

for $a = 2, 3, \cdots, p-2$.

3. To deduce the criteria of Kummer it is necessary to transform (13). Let m be an integer such that $1 < m < p$ and let $[k]$ represent the least positive residue of k_1 modulo p, where k is an integer. We have

$$mn = [mn] + mn - [mn]$$

and

$$m^s n^s \equiv [mn]^s + s[mn]^{s-1}(mn - [mn]) \pmod{p^2},$$

since $mn - [mn]$ is divisible by p. We have also

$$s[mn]^{s-1}(mn - [mn]) \equiv s(mn)^{s-1}(mn - [mn]) \pmod{p^2},$$

and therefore, if we let n range over the integers $1, 2, \cdots, p-1$, we get

$$\begin{aligned} m^s \Sigma n^s - \sum_n [mn]^s &= (m^s - 1)\Sigma n^s \\ &\equiv s m^{s-1} \sum_n n^{s-1}(mn - [mn]) \pmod{p^2}. \end{aligned} \tag{15}$$

Now, if $1 < s < p - 1$,

$$\frac{m^s - 1}{s m^{s-1}} \frac{\Sigma n^s}{p} \equiv \sum_n \frac{n^{s-1}(mn - [mn])}{p} \pmod{p}.$$

If $b_{2a-1} = 0$, $b_{2a} = (-1)^{a-1} B_a$, it is known that

$$\Sigma n^s \equiv b_s p \pmod{p^2}.$$

We then have

$$\frac{b_s(m^s - 1)}{s m^{s-1}} \equiv \sum_n \frac{n^{s-1}(mn - [mn])}{p} \pmod{p} \tag{16}$$

$$\equiv \sum_n \left[\frac{mn}{p}\right] n^{s-1} \pmod{p}$$

$$\equiv -\sum_n \left[\frac{mn}{p}\right] (p - n)^{s-1} \pmod{p}$$

$$\equiv -\sum_{\nu=1}^{m-1} \sum_{j=1}^{[\nu p/m]} j^{s-1} \pmod{p}. \tag{16a}$$

Now from (15) for $s = p - 1$ we obtain

$$-m \frac{m^{p-1} - 1}{p} \sum_n n^{p-1} \equiv \sum_n \frac{n^{p-2}(mn - [mn])}{p} \pmod{p},$$

and, noting that $\Sigma n^{p-1} \equiv -1 \pmod{p}$, we find as in the case $s < p - 1$,

$$-mq(m) \equiv \sum_{\nu=1}^{m-1} \sum_{j=1}^{[\nu p/m]} \frac{1}{j} \pmod{p}.* \tag{17}$$

---

* For other derivations of (16*a*) and (17) see the author's article in these Annals, second series, vol. 18 (1917), p. 114.

Applying (16) to (14), we have

$$\frac{b_a(1 - k^a)}{ak^{a-1}} f_{p-a}(t) \equiv 0 \pmod{p},$$

$k = 2, 3, \cdots, p - 1$ and $a = 2, 3, \cdots, p - 2$. Let k be a primitive root of p; then $1 - k^a \not\equiv 0 \pmod{p}$, and

$$b_a f_{p-a}(t) \equiv 0 \pmod{p},$$

which for a even gives the criteria of Kummer. Applying (13) and (17) to (11), we have

$$g \equiv -\frac{kyq(k)}{x + y} \pmod{p},$$

and we may state the result:

If (1) *is satisfied in integers prime to each other and z is prime to p, then it is necessary and sufficient that**

$$\prod_{\nu=1}^{k-1} \prod_{r=1}^{[\nu p/k]} (x + \alpha^{[1:r]}y) = \alpha^{-[-kyq(k)]/(x+y)}\omega^p, \tag{20}$$

$$x + y = v^p \qquad (v \text{ an integer}), \tag{21}$$

where k is any integer $1 < k < p$, and ω is an integer in $\Omega(\alpha)$.

These conditions have already been proved necessary. To prove them sufficient make the substitution (α/α^{-1}) in (20) and multiply the resulting relation by (20) and the $(k - 1)$th power of (21). We obtain

$$(x^p + y^p)^{k-1} = z_1{}^p,$$

from which (1) follows.

4. To derive Furtwängler's theorem by means of (20) set

$$\zeta^{r^f - 1/p} \equiv \left\{\frac{\zeta}{\mathfrak{P}}\right\} \pmod{p},$$

where ζ is an integer in $\Omega(\alpha)$, $\mathfrak{P}$ is an ideal prime in $\Omega(\alpha)$ which is prime to ζ and p, r^f is the norm of $\mathfrak{P}$, and $\{\zeta/\mathfrak{P}\}$ is a certain pth root of unity. Then ζ is a perfect pth power, modulo $\mathfrak{P}$, if and only if

$$\left\{\frac{\zeta}{\mathfrak{P}}\right\} = 1.$$

Let c be a rational prime factor of y in (20), if $y \not\equiv 0 \pmod{p}$. Then from (20),

$$\left\{\frac{x}{c}\right\}^{\mu(k-1)} = \left\{\frac{\alpha}{c}\right\}^{[-kyq(k)]/(x+y)}, \qquad \left(\mu = \frac{p-1}{2}\right), \tag{22}$$

where

$$\left\{\frac{x}{c}\right\} = \left\{\frac{x}{\mathfrak{P}_1}\right\}\left\{\frac{x}{\mathfrak{P}_2}\right\}\cdots\left\{\frac{x}{\mathfrak{P}_e}\right\},$$

$$c = \mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_e, \tag{23}$$

---

* Throughout this paper, whenever a fraction appears as an exponent of α, that exponent is the integer d, where d satisfies $df_1 \equiv f_2 \pmod{p}$, f_2/f_1 denoting the fraction in question.

the $\mathfrak{P}$'s being prime ideals in $\Omega(\alpha)$. Evidently

$$\{x/c\} = 1, \tag{24}$$

since if $\{x/c\} = \alpha^a$ $(a \neq 0)$, then by the substitution (α/α^m) (m prime to p) we obtain $\alpha^a = \alpha^{ma}$, whence $a = 0$. Let $k = p - 1$ in (22). We have $q(p - 1) \not\equiv 0 \pmod{p}$, and since $y \not\equiv 0 \pmod{p}$, we have using (24)

$$\left\{\frac{\alpha}{c}\right\}^g = 1 = \left\{\frac{\alpha}{c}\right\}.$$

Now in (23) the $\mathfrak{P}$'s are distinct prime ideals each of degree f, where $ef = p - 1$.* Hence

$$\left\{\frac{\alpha}{c}\right\} = \left\{\frac{\alpha}{\mathfrak{P}_1}\right\} \cdots \left\{\frac{\alpha}{\mathfrak{P}_e}\right\}$$
$$= \alpha^{e\frac{c^f-1}{p}} = 1.$$

Hence

$$\frac{c^f - 1}{p} \equiv 0 \pmod{p}, \qquad q(c) \equiv 0 \pmod{p}.$$

We have

$$x + \alpha^s y = x \pm y + (\alpha^s \mp 1)y.$$

Substituting this form in (20) we get, provided that d is a factor of $x \pm y$,

$$\Pi'\left\{\frac{(\alpha^{[1:r]} \mp 1)y}{d}\right\} = \left\{\frac{\alpha}{d}\right\}^g,$$

or, by use of (17),

$$\left\{\frac{y}{d}\right\}^{(k-1)\mu} \left\{\frac{\alpha}{d}\right\}^{-\frac{kq(k)}{2}} \Pi'\left\{\frac{\alpha^{\frac{[1:r]}{2}} \mp \alpha^{-\frac{[1:r]}{2}}}{d}\right\} = \left\{\frac{\alpha}{d}\right\}^g. \tag{25}$$

The substitution (α/α^{-1}) shows that

$$\left\{\frac{\alpha^a \mp \alpha^{-a}}{d}\right\} = 1 \qquad (a \not\equiv 0 \pmod{p}).$$

Hence (25) reduces to

$$\left\{\frac{\alpha}{d}\right\}^{\frac{k(x-y)q(k)}{2(x+y)}} = 1.$$

If $k = p - 1$, this gives, provided that $x - y \not\equiv 0 \pmod{p}$,

$$\{\alpha/d\} = 1,$$

and, as before, we find $q(d) \equiv 0 \pmod{p}$. Whence the theorem:

If

$$\frac{x^p + y^p}{x + y} = v^p,$$

where x, y and v are integers prime to each other, then $q(r) \equiv 0 \pmod{p}$,

---

* Hilbert, l. c., p. 329.

where r is any factor of xy ($xy \not\equiv 0 \pmod{p}$) and $q(r) \equiv 0 \pmod{p}$ for any factor r of x^2-y^2, provided that x^2-y^2 is prime to p. Furtwängler's theorem follows from this.

5. Kummer in his first paper referred to above applied the relation (2) to (1) for the case where x, y and z are prime to p and found

$$\prod_{s} (x + \alpha^{[1:s]}y) = \alpha^a\gamma^p,$$

where s ranges as in (2) and γ is an integer in $\Omega(\alpha)$. The integer a was not determined by him. By methods already explained we find

$$a \equiv \frac{y}{x+y}\sum_{s}\frac{1}{s} \pmod{p},$$

and[*]

$$\Sigma\frac{1}{s} \equiv -kq(k) + (k+1)q(k+1) \pmod{p}.$$

6. If in the relation (1) xyz is prime to p, then apply Wieferich's criteria $q(2) \equiv 0 \pmod{p}$ to (20) for $k = 2$. We obtain

$$\prod_{r=1}^{[p/2]} (x + \alpha^{[1:r]}y) = \omega^p.$$

Similar relations may be derived by using the criteria

$$q(3) \equiv q(5) \equiv q(11) \equiv q(17) \equiv 0 \pmod{p}.[*]$$

7. In (1), assume that z is divisible by p. By Furtwängler's theorem we note that each factor of x or y which is of the form 1 (mod p) is necessarily of the form 1 (mod p^2). Hence

$$\begin{aligned} x^p + z^p &\equiv x + z \pmod{p^3}, \\ y^p + z^p &\equiv y + z \pmod{p^3} \end{aligned}$$

and

$$x^p + y^p + 2z^p \equiv x + y + 2z \pmod{p^3}.$$

Since

$$x + y \equiv 0 \pmod{p^3},$$

we have

$$x^p + y^p + 2z^p \equiv 0 \equiv 2z \pmod{p^3}$$

or $z \equiv 0 \pmod{p^3}$. In the relation (1), x, y and z cannot all be odd. If x or y is even, then Furtwängler's theorem gives $q(2) \equiv 0 \pmod{p}$; and if $q(2) \equiv 0 \pmod{p}$, then z must be divisible by $2p^3$. By using in addition the part of Furtwängler's theorem referring to factors of $x^2 - y^2$, it may be shown that $z \equiv 0 \pmod{3p^3}$, unless $q(3) \equiv 0 \pmod{p}$.

---

[*] Vandiver, l. c., p. 114.

[†] Mirimanoff, Comptes Rendus, vol. 150 (1910), p. 206; Vandiver, Journal für die Mathematik, vol. 144 (1914), p. 314; Frobenius, Sitsungsberichte der Preuss. Akademie der Wissenschaften, vol. 22 (1914), p. 65.